A.E.

 11-689 MEM

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

Your Affiant, August Merker, being first duly sworn, deposes and states as follows:

1. I am a Special Agent with United States Immigration and Customs Enforcement, Homeland Security Investigations, hereinafter referred to as "HSI" and have been so employed since 2003. I am presently assigned to the Office of the Special Agent in Charge, Baltimore, Maryland, where I am responsible for conducting criminal investigations involving the illegal exportation of goods and services from the United States. I have prepared and executed numerous state and federal search warrants and assisted with Title III court-authorized intercepts. Further, I have gathered evidence indicative of violations of both state and federal laws, interviewed numerous suspects, witnesses and informants and have participated in the execution of search and arrest warrants in connection with the aforementioned investigations. I am currently assigned to the Counter-Proliferation Investigations Task Force where I am responsible for investigations involving export-related violations as well as associated money laundering violations in the District of Maryland. Prior to being hired by HSI, I served five years as a Police Officer in Montgomery County, Maryland.

2. This affidavit is submitted in support of application for the issuance of a search warrant for the following: a 500 GB Western Digital External Hard Drive, hereinafter referred to as "external hard drive" that is described as grey in color with black trim, Model number: WD5000MLC-00 1909A, Serial number: WXNX085D4270. The external hard drive is located at the Department of Homeland Security, U.S. Immigration and Customs Enforcement, 40 South Gay Street, Baltimore, Maryland 21201. As set forth herein, I respectfully submit that there is probable cause to believe that the items sought by this

search warrant as described in Attachment B constitute evidence of: 1) the unlawful export and attempted export of defense articles and services in violation of the Arms Export Control Act (AECA), 22 U.S.C. §§ 2778(b) and (c).

3. I have personally participated in this investigation and have witnessed many of the facts and circumstances described herein. I have also received information from witnesses employed by the effected corporation, Thales Communications Services Inc., hereafter referred to as "TCI", in relation to this investigation. The information set forth in this affidavit is based on my own observations and review of documents, or reliable information provided to me by other law enforcement personnel. I am setting forth only those facts and circumstances necessary to establish probable cause for the issuance of the requested search warrant, but have omitted nothing that would defeat a finding of probable cause. Unless otherwise indicated, all written and oral statements referred to herein are set forth in substance and in part, rather than verbatim.

Summary of Laws

I. Arms Export Control Act

4. Pursuant to the provisions of the AECA, the President of the United States is authorized to control the export and import of defense articles and services, promulgate regulations with respect to their export, and designate those items so deemed. Those items designated to be defense articles and services are set forth on the United States Munitions List (USML). By virtue of the President's delegation of his authority under § 2778, the Directorate of Defense Trade Controls (DDTC) within the Department of State (DOS) is charged with regulating the export and temporary import of defense articles and

defense services covered by the USML in accordance with the provisions of the AECA and its implementing regulations, the International Traffic in Arms Regulations (ITAR) (22 C.F.R. Parts 120-130).

5. Pursuant to 22 U.S.C. § 2778(b)(2), no defense articles or services as designated on the USML may be exported or imported without a license unless specifically provided by regulation. The ITAR states, in part, that any person who intends to export a defense article must first obtain approval from the DDTC. As such, an application for a permanent export license must be obtained prior to commencement of the export in the form of a DSP-5 ("Application/License for Permanent Export of Unclassified Defense Articles and Related Unclassified Technical Data"). Moreover, a Form DSP-83 ("Non-transfer and Use Certificate") must be duly executed and accompany all license applications for permanent export of significant military equipment. A certification letter signed by an empowered official on behalf of the intended end-user must accompany all application submissions (22 C.F.R. Part 123.1). The ITAR also require that the country designated as the country of ultimate destination on an application for an export license be the country of end-use (22 C.F.R. Part 123.9). Additionally, a Form DSP-83 stipulates that a foreign consignee or foreign end-use will not re-export, resell or otherwise dispose of significant military equipment enumerated in an application outside the country named as the location of intended end-use (22 C.F.R. Part 123.10).

II. Probable Cause

6. On or about January 2, 2011, your affiant received information from TCI, Clarksburg, Maryland, that an employee identified as Alan HUYNH, was terminated by TCI, effective December 30, 2010, as a result of having committed several TCI security

AEE.

violations against company policy.

a. TCI is a pioneer of software-defined radio (SDR) technology and a global leader in the development, manufacture, and support of innovative communications systems for warfighters and first responders. TCI is headquartered in Clarksburg, Maryland and has four Maryland locations as well as in-theater maintenance and repair depots supporting U.S. troops in Kuwait and Afghanistan. The company's products are developed and manufactured at its Maryland facilities.

7. Alan Huynh was an employee of TCI and worked as a Diagnostic Test Technician in the Customer Service Department (CSD). His primary job was to maintain and repair the circuit boards in the MultiBand Inter/Intra Team Radio, hereafter referred to as "MBITR". The MBITR contains a classified encryption chip. HUYNH was responsible for testing the radios to determine if the encryption chip holds the classified key or does not hold the key. In addition, HUYNH was responsible for diagnosing radios that were no longer functional. HUYNH's diagnostic procedures involved testing the radio circuit boards before the encryption chip was integrated, testing the circuit boards after the encryption chip was integrated and finally, testing the encryption chip itself in an effort to locate the specific problem area within the non-functioning radios. HUYNH did not do any work that would provide him access to the classified encryption keys within the chip. HUYNH did have a "secret" security clearance while he was employed with TCI.

8. On December 22, 2010, at approximately 13:55 hours, the TCI computer network Virus Protection software reported that malware had been detected as a "hacktool" on the TCI network. At approximately 14:00 hours, the information concerning this incident/network intrusion was forwarded to TCI Information Technology (IT) Director and

an investigation began of the incident both remotely and at the Personal Computer (PC) in question. TCI's Virus Protection software identified the attempted intrusion location as "B1CSDLAB38" which is a PC located in the TCI Customer Service Lab. The user, Alan Huynh "ahuynh" was logged into the PC at the time the network virus protection software recognized the "hacktool" on the TCI network. TCI Information Systems Security Officer (ISSO), Chris La Scola investigated the incident 5 minutes after the detection.

9. ISSO La Scola immediately responded to HUYNH's TCI PC/work station in an effort to ascertain what caused the notification that "hack tools" had been connected to the TCI network. La Scola observed HUYNH sitting at location "B1CSDLAB38" and asked HUYNH what he was doing at his work station to cause the TCI network notification. HUYNH denied any knowledge of what caused the notification and stated that perhaps his radio on his desk had caused some kind of interference.

10. Consequently, HUYNH's denial of any knowledge or participation in causing the security violation at his work station resulted in his immediate Supervisor, Dave Kukor being notified which led Kukor to address the security violation with HUYNH directly. Eventually, HUYNH admitted to Kukor that he was in possession of a personally-owned external hard drive and that he had connected it to the TCI network at his personal work station in the lab where he was working. Kukor asked HUYNH to turn over the external hard drive to Kukor. HUYNH complied with the request, without incident.

11. Subsequently, the external hard drive, identified as a 500 GB Western Digital External Hard Drive described as grey with black trim, Model number WD5000MLC-00 1909A, Serial number WXNX085D4270, was delivered to ISSO La Scola to investigate. After doing a basic investigation of the drive contents, an in-depth investigation was

AEG.

initiated per the instructions of the TCI-IT Director because of the nature and amount of data found on the storage device. ISSO La Scola completed the investigation and documented the results in an IT Security Incident Report which was eventually forwarded to your affiant.

12. The incident report revealed that a large amount of Export-Controlled, TCI company data including schematics, software and test data, relating to TCI encrypted radios, used by U.S. troops overseas was stored on HUYNH's personally-owned, unprotected, External Hard Drive (storage device). This storage device was also found to contain IT Security (Hacking) Pre-Boot Security Tool Suites, Password Crackers, Software Activation Crackers, Malware, Internet Proxy Tools and Site Lists, and Hacker Tutorial Videos.

13. The following additional information is from ISSO La Scola's IT Security Incident Report based on the forensic analysis of HUYNH's personally-owned unprotected, external hard drive. "Several folders contained files that are an IT security concern. Many tools used for compromising computer security along with instructional videos on how to "hack" computer systems were found". Below is the list of folders from the external hard drive where data was found. These folders also contain subfolders containing similar data.

a. E:\KUWAIJOB\Alan\Hiren'BootCD9.3(D)- This is a pre-boot software suite that contains several hacking tools that could compromise TCI security.

b. E:\KUWAIJOB\download\1000 Hacker Tutorials (2008) – Instructional videos on hacking computer systems.

c. E:\KUWAIJOB\Kuwait Pic\New Folder – Contains several different

MAC changers, Network Sniffers, and Hacked Firmware for Cable Modems.

d. E:\KUWAIJOB\New Folder – Contains several different MAC changers, Network Sniffers, and Hacked Firmware for Cable Modems

e. E:\KUWAIJOB\Newstorage\Newstorage1\limewire – Contains an Internet File Sharing application along with cracks for the Microsoft Windows OS to disable activation.

f. E:\KUWAIJOB\stuff\Software – Another folder that contains the several of the tools mentioned. Looks to be a back up or duplicate folder.

g. E:\MioNet\software – Contains several Microsoft Windows OS cracks to disable activation.

14. According to La Scola's report, tools and lists used to avoid web filtering and monitoring were also found on HUYNH's external hard drive. In some cases, the tools were included in software suites used to upload/download large files to the internet. La Scola reported that it appeared that no traces of the use of these sites or tools were found on the TCI network. Below is the list of folders where this data was found on HUYNH's external hard drive. These folders also contain subfolders containing similar data.

a. E:\KUWAIJOB\Lam folder\SOFTWARES – Contains an installer for proxy software used to avoid web filtering.

b. E:\KUWAWIJOB\Newstorage\Newstorage1\Software – Contains a proxy list text file with sites that can be used to avoid web filtering. Also contains a program called file splitter and joiner. This software can be used to modify files and folders that would otherwise be detected as malicious or sensitive then reconstruct them later to be used.

A.E.E.

c. E:\KUWAIJOB\Newstorage1\Software\greatesttools\greatest tools – Contains a software suite used to manipulate/download/upload large files. A proxy switcher tool is also included to avoid detection by web filtering and monitoring.

d. E:\MioNet\software\software – Contains an installer for proxy software used to avoid web filtering.

These items are important because the hacking tools and proxy software used to avoid web filtering may be used to help someone access computer programs from a companies computer system that their clearance does not give them access to.

15. Additionally, La Scola's report alleges that a large amount of pirated (illegally obtained) movies and software were found on HUYNH's external hard drive. The software contains serial key generators and software cracks to allow the use without proper purchase. Below is the list of folders where such data was found. These folders also contain subfolders containing similar data.

a. - E:\KUWAIJOB\download

b. - E:\KUWAIJOB\Film Collection

c. - E:\KUWAIJOB\Lam Folder\SOFTWARES

d. - E:\MioNet\software

e. - E:KUWAIJOB\stuff

f. - E:\KUWAIJOB\Microsoft Office 2010

g. - E:\KUWAIJOB\Window 7 Pro

It is possible that some of the pirated software may be from other defense contractors and that software maybe ITAR controlled.

16. La Scola reported that a folder containing very detailed schematics for

A.E.

various non-TCI computer products was found on HUYNH's external hard drive. Some of the documents were labeled as proprietary data. La Scola was not able to determine whether or not these schematics were acquired legally. Below is the list of folders where such data was found. These folders also contain subfolders containing similar data.

a. - E:\KUWAIJOB\Lam folder\schematics

17. Further, HUYNH conceded to Dave Kukor that his external hard drive was used to transport company data to his residence as well as outside of the United States.

b. HUYNH has traveled to Kuwait on two occasions to work at the TCI repair depot in support of TCI contracts with the U.S. Army to repair the MBITR, which is encrypted and controlled for export by the ITAR. HUYNH was first temporarily assigned to work at the TCI repair depot in Kuwait from June 29, 2009 through November 24, 2009. HUYNH's second assignment in Kuwait was from January 4, 2010 through January 29, 2010.

18. Kukor stated to your affiant that in June of 2009 before HUYNH left for Kuwait, HUYNH told him that he was going to take the schematic of the MBITR over to Kuwait so that he could repair the radios. Kukor told HUYNH that there was no need to take a schematic of the MBITR over to Kuwait because the repair facility in Kuwait just swaps out boards and does not try to repair the circuits that may be faulty in the radio. Faulty circuit boards in the radio are simply exchanged, due to time constraints instead of attempting to actually repair the radios on-site

19. HUYNH did not ever have permission from TCI to travel outside the United States with any external hard drives, storage devices or TCI technical data. In the event

A.E.E.

that permission had been given to travel outside of the United States with TCI technical data, a TCI "Iron-Key", hard drive or otherwise approved storage device would have been required. HUYNH has never been issued any of the aforementioned TCI storage devices.

20. On December 30, 2010, TCI terminated HUYNH. In the process of terminating HUYNH, TCI filled out an Employee Warning Report. This form is used for all employees who have violated TCI policy. A summary of the facts are listed as follows in the "Facts or Events" section of the report: "TCI proprietary data, such as detailed product schematics, was stored on an unapproved, unencrypted, storage device comingled with hacking tools, malware, and miscellaneous illegal content. Additionally, proprietary data from other companies were stored on this device. While we were unable to determine if TCI Company data had been compromised, it is reasonable to assume that since the drive contained malware (that was most likely introduced when obtaining hacking tools) the data on the drive may have been compromised. Further, Alan conceded to Dave Kukor that this drive was used to transport company data to home and overseas while working at the depot. IT is unable to determine if company data was compromised while this drive was off TCI's network. Numerous hacking tools and instructional videos were found on the drive. While there is no evidence to support Alan used these tools on TCI's network, it's reasonable to assume that based on the type of tools found, Alan's intent was to learn how to compromise TCI's, or other private networks, if he hasn't already. Even if Alan did not actively hack TCI's network, considering he downloaded hacking tools infected with malware, it's reasonable to assume that the authors of the hacking tools may have tried to hack TCI's network. Illegal content, such as pirated movies and applications, were found on the drive."

21. The bottom of the report states "I have read and understand the information presented in this Employee Warning Report". The report is signed by Alan HUYNH and dated December 30, 2010.

22. On June 11, 2007 Alan HUYNH signed an employee Invention assignment and confidentiality agreement. HUYNH also signed a non-disclosure agreement. The last sentence of the non-disclosure agreement reads as follows "Consultant agrees to comply with all applicable laws and regulations concerning export control of the data received from company".

23. On February 14, 2011 the Department of State, Directorate of Defense Trade Controls (DDTC) issued a license determination for the TCI MBITR and stated that it is controlled By the ITAR. The MBITR is found on the United States Munitions List Article Category: XI (b).

24. Email accounts have been identified that HUYNH could have used to export the information contained on his external hard drive as a result of a review of HUYNH's TCI employee email account. Specifically, the review of the email account revealed that HUYNH is associated with four different e-mail accounts. Two are believed to be personal email accounts and two are believed to be military accounts that HUYNH likely utilized while working at the TCI repair depot in Kuwait. These email accounts have been identified as follows; alan.l.huynh@kuwait.swa.army.mil , huynh.alan@ymail.com , alan.huynh2@us.army.mil , alanhuynhrealtor@yahoo.com.

III. Conclusion

25. HUYNH downloaded and subsequently saved to his personally-owned external hard drive, TCI technical data and schematics, relating to the MBITR radio as well

as other TCI radios that are used in-theatre by the U.S. Army as well as other Department of Defense entities for secure, encrypted communications purposes. Further, these radios and related technical data are export controlled by the ITAR and require the issuance of a valid Department of State license before any export from the United States can be affected. As described in this affidavit, HUYNH admitted to taking this external hard drive out of the United States, i.e., affecting an export, without the appropriate approvals and without securing the data on an approved TCI storage device. A forensic search of HUYNH's external hard drive will show the exact date and time that HUYNH downloaded the export controlled information from the TCI computer network to his personally owned external hard drive, as well as the dates and times that data was accessed. The forensic search will also allow an examination of the aforementioned proprietary data described in the TCI IT report that HUYNH saved to his personally-owned external hard drive in an effort to determine if the proprietary data is potentially export controlled by the ITAR. This search will also provide when that data was downloaded and saved to HUYNH's external hard drive as well as the times that data was accessed.

26. HUYNH is associated with 4 different e-mail accounts which may have been used as a vehicle to export ITAR controlled data. Your affiant is currently working with a Special Agent from the Defense Criminal Investigative Service to get access to the two military e-mail accounts cited earlier in this affidavit. Your affiant has sent an Administrative Export subpoena to Yahoo! Inc. to identify the subscriber information for both alanhuynhrealtor@yahoo.com and huynh.alan@ymail.com. Your affiant has also sent a retention letter to Yahoo! Inc. so that all the data for the above referenced yahoo! e-mail accounts will be retained. Your affiant anticipates requesting a search warrant for both e-

A.E.

mail accounts. Based upon the information above, your affiant believes that there is probable cause to support the search of the 500 GB external hard drive, serial number WXNX085D4270 and that the contents of the aforementioned external hard drive constitutes fruits, instrumentalities and evidence of violations of 22 U.S.C. § 2778 (b) and (c).

Your affiant has signed this document under oath as to all assertions and allegations contained herein and states that its contents are true and correct to the best of his knowledge.

August Merker, Special Agent
Immigrations & Customs Enforcement
Homeland Security Investigations

Sworn and subscribed to before me this 25TH day of February, 2011.

Mildred Methvin
United States Magistrate Judge

ATTACHMENT A

500 GB Western Digital External Hard Drive, is described as grey in color with black trim, Model number: WD5000MLC-00 1909A, Serial number: WXNX085D4270 which is currently located at the office of the Department of Homeland Security, Immigration and Customs Enforcement, 40 South Gay Street, Room 322, Baltimore, Maryland.

A2.E

ATTACHMENT B

The following is a list of items to be searched for and, if found, seized from the External Hard Drive as fully described in Attachment A:

1. Any and all notes, documents, records, or correspondence pertaining to the unlawful export and attempted export of defense articles and services in violation of the Arms Export Control Act (AECA), 22 U.S.C. §§ 2778(b) and (c);

2. Any and all correspondence identifying persons transmitting, receiving, possessing, or exporting defense articles and services in violation of the Arms Export Control Act (AECA)

3. Evidence of internet postings referencing items controlled by the Arms Export Control Act;

4. Any and all proprietary data such as schematics, software, and test data owned by TCI or any other proprietary data from Non-TCI Companies.

5. Any and all records, documents and correspondence reflecting or referencing financial transactions, including but not limited to, bank records, bank statements, budget documents, loan documents, loan applications, financial correspondence, rental agreements, credit card statements and bills, debit and prepaid card statements and bills, frequent customer-type card statements (such as Best Buy Reward Zone), cancellation notices, purchase receipts, customer complaint documents, confirmation notices, acceptance letters, as well as records, document or correspondence that is evidence of income and earning.

6. If after performing these procedures, the directories, files or storage areas do not reveal evidence of exporting defense articles and services in violation of the Arms Export Control Act (AECA) or other criminal activity, the further search of that particular directory, file or storage area, shall cease.

A55

ATTACHMENT C

Description of Methods to be Used for Searching Computer-Related Items

This warrant authorizes the search of electronically stored information. The search shall be conducted pursuant to the following protocol in order to minimize to the greatest extent possible the likelihood that files or other information for which there is not probable cause to search are viewed.

With respect to the search of any digitally/electronically stored information seized pursuant to the instant warrant as described in Attachments B hereto, the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized;

c. physical examination of the storage device, including surveying various file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized;

d. opening or reading portions of files in order to determine whether their contents fall within the items to be seized;

e. scanning storage areas to discover data falling within the list of items to be seized, to possibly recover any such deleted data, and to search for and recover files falling within the list of items to be seized; and/or

f. performing key word searches through all electronic storage areas to determine whether occurrence of language contained in such storage areas exist that are likely to appear in the evidence to be seized.